Homework #7

Due **Wednesday, March 11** in Gradescope by **11:59 pm ET**

READ Sections 5.3, 5.4 in Cox and the **Separability and Primitive Elements** handout

WATCH 1. Video 17: Separable Degree, Part 1 (35:31)

2. Video 18: Separable Degree, Part 2 (12:10)

WRITE AND SUBMIT solutions to the following problems.

Problem 1. (10 points) Cox, Section 5.3, Exercise 10a:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension.

Prove that L/F is purely inseparable if and only if for every $\alpha \in L$,
the minimal polynomial of α over F is of the form $x^{p^e} - a$ for some $e \geq 0$ and some $a \in F$.

[Cox suggests using Proposition 5.3.16.]

Problem 2. (8 points) (not from Cox):
Let $L/M/K$ be finite extensions of characteristic p fields. If L/K is purely inseparable, prove that both M/K and L/M are purely inseparable.

[**Suggestion**: use Problem 1 above, i.e. Cox 5.3, Exercise 10a]

Problem 3. (9 points) Cox, Section 5.3, Exercise 10b:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension. If L/F is purely inseparable, prove that $[L : F]$ is a power of p.

[**Suggestion**: use Problems 1 and 2 above.]

Problem 4. (9 points) Cox, Section 5.3, Exercise 13:
Let F be a field of characteristic $p \geq 2$, and let L/F be a finite extension with $p \nmid [L : F]$. Prove that L/F is separable.

Problem 5. (8 points) Cox, Section 5.3, Exercise 14: Let $L/K/F$ be algebraic extensions. Suppose that L/F is separable. Prove that both L/K and K/F are separable.

[**Note**: We used this fact to prove other results later, including the fact that this implication is actually an if-and-only-if. Obviously, you cannot use any of those subsequent results here.]

Problem 6. (14 points) Cox, Section 5.3, Exercise 16:
Let F be a field of characteristic $p \geq 2$, let $a \in F$, and let $f = x^p - x + a \in F[x]$.

(a) Prove that f is separable.

(b) Let α be a root of f in some extension L of F. Prove that $\alpha + 1$ is also a root of f.

(c) Use part (b) to prove that f splits completely over $F(\alpha)$.

(d) Use Theorem 5.3.15(a) to prove that $F(\alpha)/F$ is normal and separable.

[**FYI**: The polynomial $f = x^p - x + a$ is called an *Artin-Schreier* polynomial, and $F(\alpha)/F$ is an Artin-Schreier extension. Artin-Schreier theory provides an appropriate separable replacement for the inseparable extension $F(\sqrt[p]{a})/F$ in the case that char $F = p$. See also HW 3, Problem 3.]

(continued next page)

Problem 7. (14 points) Cox, Section 5.4, Exercise 2:
Let F be a finite field, and let L/F be a finite extension.

(a) Prove that L is also a finite field.

(b) By Proposition A.5.3, since L is a finite field, its multiplicative group (i.e., $L^\times = L \setminus \{0\}$ under the operation of $\cdot$) is a cyclic group. Let $\alpha \in L^\times$ be a generator of this cyclic group. Prove that $L = F(\alpha)$.

(c) Let $m = |L| - 1 = |L^\times|$ and $f(x) = x^m - 1 \in F[x]$. Prove that for all $0 \le i \le m-1$, we have $f(\alpha^i) = 0$. Then conclude that

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1}).$$

(d) Use part (c) to prove that α is separable over F. [Thus, $L = F(\alpha)$, and L/F is separable.]

Problem 8. (20 points) Cox, Section 5.4, Exercise 4, variant:
As in Example 5.4.4, let k be a field of characteristic $p \ge 2$, let $F = k(t,u)$, and let L/F be the splitting field of $f(x) = (x^p - t)(x^p - u) \in F[x]$, where $\alpha^p = t$ and $\beta^p = u$.
[That is, $\alpha = \sqrt[p]{t}$ and $\beta = \sqrt[p]{u}$.]

(a) Prove that $L = F(\alpha, \beta)$.

(b) Let $E = F(\alpha)$. Prove that $g(x) = x^p - t$ has no roots in F, and that $h(x) = x^p - u$ has no roots in E.

(c) Use part (b) to prove that $[L : F] = p^2$.

(d) Prove that for all $\gamma \in L \setminus F$, we have $[F(\gamma) : F] = p$.

(e) Prove that L/F is purely inseparable.

[Note that parts (c) and (d) together show that L/F is an example of a finite extension that does *not* have a primitive element.]

Problem 9. (8 points) Cox, Section 5.4, Exercise 5:
With notation as in Problem 8 above (Cox 5.4 Exercise 4), for each $\lambda \in F$, define $K_\lambda = F(\alpha + \lambda\beta)$. Clearly we have $L/K_\lambda/F$. Suppose that there exist $\lambda \ne \mu \in F$ such that $K_\lambda = K_\mu$.

(a) Prove that $\alpha, \beta \in K_\lambda$.

(b) Conclude that $K_\lambda = L$, and explain why this, together with the results of Problem 8, yields a contradiction.

[It follows that the fields K_λ are all distinct. Since F is infinite, this means that there are infinitely many different fields between L and F, even though L/F is a finite extension.]

Optional Challenges (do NOT hand in): Cox Problems 5.4 #6,7

Questions? You can ask in:

Class: MWF 9:00am – 9:50am, SCCE C101

My office hours: in my office (SMUD 406):
Mon 2:00–3:30pm
Tue 1:30–3:15pm
Fri 1:00–2:00pm

Also, you may email me any time at `rlbenedetto@amherst.edu`